CISO MAG

beyond cybersecurity

Volume 5 | Issue 10 | October 2021

44

Cybersecurity's Role In Keeping Blockchain Secure

Sriram Tarikere
Senior Director
Alvarez & Marsal's Global
Cyber Risk Services (New York)

INSIGHT

72

Implementing Blockchain for Business

SURVEY REPORT

BLOCKCHAIN UNDER ATTACK

How Adversaries are Manipulating Cryptos, DeFi and the Blockchain Ecosystem

CISO MAG

beyond cybersecurity

EDITORIAL ADVISORY BOARD

CISO MAG established an **Editorial Advisory Board** with the foremost innovators and thought leaders in the cybersecurity space. Board members offer the CISO MAG editors advice regarding the magazine as well as suggest the strategic direction it should follow. It includes shaping our editorial content, identifying important topics and special issues, moderating discussions, vetting technical content, and updating the magazine's presence by creating and implementing different initiatives.

The Advisory Board members are "**active**" participants and contribute to CISO MAG regularly. They contribute in either of the following ways:

- Editorial strategy
- Writing articles
- Exclusive quotes for editorial stories
- Vetting surveys and technical content
- Podcasts, webinars, video, and text interviews

Carolyn Crandall

Chief Security Advocate
Attivo Networks

Carolyn Crandall is the Chief Security Advocate at Attivo Networks, the leader in preventing identity privilege escalation and detecting lateral movement attacks. She has worked in high-tech for over 30 years and has been recognized as a top 100 women in cybersecurity, a guest on Fox News, and profiled in the Mercury News. She is an active speaker on security innovation at CISO forums, industry events, and technology education webinars. Carolyn also co-authored the book *Deception-Based Threat Detection: Shifting Power to the Defenders.*

Vandana Verma

Security Relations Leader
Snyk

Vandana is a Security Relations Leader at Snyk with a current focus on DevSecOps. She has extensive experience in Application Security, Vulnerability Management, SOC, Infrastructure Security and Cloud Security. Vandana is a seasoned speaker and trainer. She presented at various public events ranging from Global OWASP AppSec events to BlackHat events, to regional events such as BSides events in India. She is on the OWASP Global Board of directors (Vice-Chair). She also works in various communities towards diversity initiatives such as InfosecGirls, InfosecKids and WoSec. She is a recipient of multiple awards and is listed as one of the top women leaders in technology and cybersecurity in India by Instasafe.

Favour Femi-Oyewole

Global Chief Information Security Officer (CISO)
Access Bank Plc.

Favour Femi-Oyewole has over 23 years of experience managing all aspects of Information Technology with vast knowledge in Enterprise IT Security, Information Technology, IT Governance, Information Security best practices, Cyber Security, Business Continuity, and Risk Management, especially in dynamic, demanding large scale environments. She is also regarded as the first female COBIT 5 Assessor certified in Africa, the first female in Africa to be a Blockchain Certified Professional, and the first woman to win the Global Certified CISO (C|CISO) of the Year 2017. She is a Certified ISO 27001:2013 Lead Implementer Trainer and an Alumni of Harvard Kennedy School (HKS) - Harvard University and Massachusetts Institute of Technology (MIT). She is a member of the Cybercrime Advisory Council in Nigeria with the Mandate of implementing Cybersecurity for all sectors in Nigeria and the pioneer Chair of the Standard and Evaluations Committee. She is a Fellow of the British Computer Society (BCS), The Chartered Institute for IT. She serves as a member of the Global C|CISO Advisory Board and the Information Security woman of the Year 2021 in Nigeria.

Tari Schneider

C|CISO, CRISC, MCRP, ITILF – Cybersecurity Architect, Author & C|CISO Instructor **EC-Council**

Tari Schreider - C|CISO, CRISC, MCRP, ITILf – is a Cybersecurity Architect, Author, Researcher, C|CISO Instructor at EC-Council, and Strategic Advisor at Aite-Novarica Group covering the cybersecurity industry. He is the author of two Amazon top sellers Building an Effective Cybersecurity Program and Cybersecurity Law, Standards and Regulations. He is also a cybersecurity strategist and C|CISO Master Course instructor passionate about making CISOs the smartest people in the room. Tari consults with organizations to guide the transformation of their cybersecurity programs to obtain regulatory compliance and stave off cyberattacks.

Dr. Charlotte M. Farmer

Independent Director

Charlotte is an experienced Director and Board Member with proven value creation across blue chip companies and top-tier general management consulting firms. Over the last 25 years, she has served as Board Chair, Committee Chair, or Board Advisor to 16 non-governmental organization (NGO) boards. Currently, she serves as Board Chair of a tech start-up and advisor to a private equity company in The Carlyle Group portfolio. Her board expertise includes strategy, governance, and turnaround with proven results building high-performing, growth organizations. Her leadership roles in high-tech manufacturing, global operations, finance, and digital transformation would also be an asset to companies eager to expand their footprint or companies in need of turnaround guidance.

Stan Meirzwa

M.S., CISSP, Director
Kean University Center for Cybersecurity

Stanley Mierzwa is the Director of, Center for Cybersecurity at Kean University in the United States. He lectures at Kean University on Cybersecurity Risk Management, Cyber Policy, Digital Crime and Terrorism, and Foundations in Cybersecurity. Stan has over 15 published research publications and is a peer reviewer for the International Journal of Cybersecurity Intelligence and Cybercrime, Online Journal of Public Health Informatics and an Editorial Review Board member for the International Association for Computer Information Systems. He is a Certified Information Systems Security Professional (CISSP) and member of several associations, including the FBI Infragard, IEEE, and (ISC)^2. He is a board member (Chief Technology Officer) of the global pharmacy education non-profit, Vennue Foundation. Stan holds an MS in Management with a specialization in Information Systems from the New Jersey Institute of Technology and a BS in Electrical Engineering Technology from Fairleigh Dickinson University.

John Kindervag

Senior Vice President Cybersecurity Strategy
ON2IT and ON2IT Global Fellow

John Kindervag joined ON2IT in March of 2021 as Senior Vice President Cybersecurity Strategy and ON2IT Global Fellow. He spent the previous four years at Palo Alto Networks as Field CTO. Before Palo Alto Networks, John spent eight and one-half years at Forrester Research as a Vice President and Principal Analyst on the Security and Risk Team. John is considered one of the world's foremost cybersecurity experts. He is best known for creating the revolutionary Zero Trust Model of Cybersecurity.

Muhammad Tariq Ahmed Khan

Head of Information Security Audit,
Internal Audit Department, **Riyad Bank, KSA.**

Muhammad Tariq Ahmed Khan is Head of Information Security Audit, Internal Audit Division, Riyad Bank, KSA. He has over 21 years of experience in the Banking industry, in areas such as Information Technology, Cyber & Information Security, Business Continuity Management & Disaster Recovery and related Audits. He has a solid understanding and application of Risk-Based Audit methodology, ISMS (ISO 27001), ISO 22301, NIST and COBIT, IT & Information Security regulatory compliance.

He is a double Graduate (Finance and Computer Science) with one Master's Degree in Computer Science. In addition, he holds a number of professional certifications such as CISA, CISM, CRISC, CDPSE, CISSP, PMP, CEH, ISO 27001 ISMS Lead Implementer & ISO 22301 BCMS.

Tariq has published articles on different topics of Cyber & Information Security and IT Audit and also spoken at regional and international seminars and conferences.

Zachery Mitcham

MSA, CCISO, CSIH, VP and Chief Information Security Officer, **SURGE Professional Services-Group**

Zachery S. Mitcham is a 20-year veteran of the United States Army where he retired as a Major. He earned his BBA in Business Administration from Mercer University Eugene W. Stetson School of Business and Economics. He also earned an MSA in Administration from Central Michigan University. Zachery graduated from the United States Army School of Information Technology where he earned a diploma with a concentration in systems automation. He completed a graduate studies professional development program earning a Strategic Management Graduate Certificate at Harvard University extension school. Mr. Mitcham holds several computer security certificates from various institutions of higher education to include Stanford, Villanova, Carnegie-Mellon Universities, and the University of Central Florida. He is certified as a Chief Information Security Officer by the EC-Council and a Certified Computer Security Incident Handler from the Software Engineering Institute at Carnegie Mellon University. Zachery received his Information Systems Security Management credentials as an Information Systems Security Officer from the Department of Defense Intelligence Information Systems Accreditations Course in Kaiserslautern, Germany.

Narendra Sahoo

Founder and Director, **VISTA InfoSec**

Narendra Sahoo (PCI QSA, PCI QPA, PCI SSFA, CISSP, CISA, CRISC and CEH) is the Founder and Director of VISTA InfoSec, a global Information Security Consulting firm, based in the U.S., UK, Singapore & India. Mr. Sahoo holds more than 25 years of experience in the IT Industry, with expertise in CyberSecurity Risk Consulting, Assessment, and Compliance services. VISTA InfoSec specializes in Cyber Security audit, consulting, and certification services which include PCI DSS Compliance & Audit, PCI PIN, PCI SSF, SOC1/2, GDPR Compliance and Audit, HIPAA, CCPA, NESA, MAS-TRM, PDPA, PDPB to name a few. The company has for years (since 2004) worked with organizations across the globe to address the Regulatory and Information Security challenges in their industry. VISTA InfoSec has been instrumental in helping top multinational companies achieve compliance and secure their IT infrastructure.

Sunil Varkey

VP
Forescout

Sunil Varkey has over 26 years of Security leadership experience, with large global corporates in banking, telecoms, ITES, software, and manufacturing. At Forescout he is involved in security strategy, innovation, and stakeholder engagements, prior to this he led Cyber Security Assessment and Testing for HSBC, he also worked with Symantec as CTO and Strategist, Wipro as Global CISO and Fellow, as Head of Security and Privacy at Idea Cellular, and in GE, Barclays and SABB.

Dick Wilkinson

Chief Technology Officer
Proof Labs

Dick Wilkinson is the Chief Technology Officer at Proof Labs. He also served as the CTO on staff with the Supreme Court of New Mexico. He is a retired Army Warrant Officer with 20 years of experience in the intelligence and cybersecurity field. He has led diverse technical missions ranging from satellite operations, combat field digital forensics, enterprise cybersecurity as well as cyber research for the Secretary of Defense.

AJ Yawn

Founder and CEO
ByteChek

AJ Yawn is a seasoned cloud security professional that possesses over a decade of senior information security experience with extensive experience managing a wide range of cybersecurity compliance assessments (SOC 2, ISO 27001, HIPAA, etc.) for a variety of SaaS, IaaS, and PaaS providers. AJ is a SANS Institute instructor and currently teaches the SEC557: Continuous Automation for Enterprise and Cloud Compliance.

AJ is a Founding Board member of the National Association of Black Compliance and Risk Management professions, regularly speaks on information security podcasts, events, and he contributes blogs and articles to the information security community including publications such as CISOMag, InfosecMag, HackerNoon, and (ISC)².

Christina Gagnier

Shareholder
Carlton Fields' Los Angeles office

Christina Gagnier, a shareholder in Carlton Fields' Los Angeles office, is an experienced technology lawyer whose practice focuses on cybersecurity and privacy, blockchain technology, international regulatory affairs, technology transactions, and intellectual property. She advises clients on digital strategy to help them navigate uncharted legal territory, and guides a variety of technology companies and consumer brands through emerging legal and policy issues such as digital currency, the sharing economy, network neutrality, and the ever-changing area of consumer privacy law.

Christina has served on notable committees and task forces, including the Federal Communication Commission's Consumer Advisory Committee and the California attorney general's Cyber Exploitation Task Force. Outside her practice, Christina is an adjunct professor at the University of California, Irvine School of Law, where she serves as clinical faculty for the Intellectual Property, Arts, and Technology Clinic.

EC-Council

codered FROM EC-COUNCIL

Subscribe Now to CodeRed Pro for Just

$1

Access **240+ Premium Courses** in Cybersecurity

Unlimited Access Guaranteed!

CodeRed Pro Exclusives	$1 Subscription	Monthly/ Annual Subscription
Access to 240+ premium courses	✓	✓
Courses co-developed by academia & industry experts	✓	✓
Access to over 100 final assessments	✓	✓
Access to over 10,000 practical videos	✓	✓
Course recommendations based on career goals and watch history	✓	✓
Daily goal setting to help you be consistent in learning	✓	✓
Favorites list to add lessons that interest you the most	✓	✓
The ability to add and save notes on your lessons	✓	✓
Globally recognized certificate when you complete the course to show off your skills	✓	✓

Quality Assured by CodeRed Community

50K

Professionals are improving their cybersecurity skills with CodeRed

98%

Satisfaction rate from our learners

4.5/ 5.0

Average customer ratings on our courses

Our best trial offer is here, but it may not be for long.

CodeRed, EC-Council's continuous learning platform, offers premium in-demand cybersecurity courses designed for busy working professionals and career starters.

CodeRed Pro Annual and Monthly plans are now available for just $1 for a 7-day unlimited access.

Subscribe to CodeRed Pro Monthly or Annual plan now for just $1 for 7 days. Cancel anytime.

Get Started with CodeRed Pro – Monthly for Just $1

Trending Now

Get Started with CodeRed Pro – Annual for Just $1

EC-Council

24 Hacking Challenges

100% Performance based Course! | No Death by Powerpoint! | Learn by Doing! | Step By Step Video Instruction

W|AHS

Web | Application Hacking & Security

100% Hands-On

Challenge-Based Learning

Comprehensive Knowledge on OWASP TOP 10

Excel in Web Application Security Testing with EC-Council Web Application Hacking & Security

Become a Certified Web Application Security Associate | Professional | Expert

REGISTER TODAY

If you are a cyber or tech professional who is interested in learning or recommending mitigation methods to a myriad of web security issues and want a pure hands-on program, then this is the course you have been waiting for.

Test your skills and learn to hack applications with Web Application Hacking and Security. Whether you are a beginner, or an experienced ethical hacker, Web Application Hacking and Security course offers something for all skill levels.

CISO
MAG
beyond cybersecurity

Volume 5 | Issue 10
October 2021

Image credits: Shutterstock & Freepik
Illustrations, Survey Design, Cover & Layouts by: Jeevana Rao Jinaga

* Responsible for selection of news under PRB Act. Printed & Published by Brian Pereira, E-Commerce Consultants Pvt. Ltd.,
The publishers regret that they cannot accept liability for errors & omissions contained in this publication, howsoever caused. The opinion & views contained in this publication are not necessarily those of the publisher. Readers are advised to seek specialist advice before acting on the information contained in the publication which is provided for general use & may not be appropriate for the readers' particular circumstances. The ownership of trade marks is acknowledged. No part of this publication or any part of the contents thereof may be reproduced, stored in a retrieval system, or transmitted in any form without the permission of the publishers in writing.

EDITOR'S NOTE

DARK SIDE OF THE COIN AND BLOCK

Brian Pereira
Editor-in-Chief

When the first blockchain transaction was conducted on Jan 3, 2009, the business world noticed and acknowledged blockchain as a disruptive technology. Many saw it as a solution for bringing trust and transparency to digital environments. It was looked at as a technology for expanding trade, enabling new markets, and providing more transparency in business processes.

In the decade that followed, organizations in various industries undertook blockchain pilots to explore business value derived from the blockchain. Through various experiments, they were hoping to solve counterfeiting and fraud, challenges with data management, and inefficiencies caused by opaque, manual processes and outdated systems of records.

Gartner estimates that blockchain could generate as much as $3.1 trillion in new business value by 2030 – half of it by 2025, which is just four years away. There will be enormous demand for applications that are designed for operational improvement, says Gartner.

From a security standpoint, Encryption and Immutability stand out from the five elements of blockchain. The other three elements being Distribution, Tokenization, and Decentralization. *(The Real Business of Blockchain, David Furlonger and Christophe Uzureau, HBR Press.)*

THE DARK SIDE

While blockchain enables secure transactions, the technology can also be misused. I am not saying there are vulnerabilities in the technology that can be exploited. Blockchain technology by itself is rock stable and watertight. Rather, there are weaknesses in the supporting infrastructure and ecosystem.

In our cover story on page 52, **Srinivas Balantrapu**, Director and Head of India-Cyber Security and Blockchain COE, Conduent, writes about the promising applications of blockchain and the dark side or misuse of DeFi (decentralized finance). He offers details about how malicious actors target crypto exchanges and how their greed leads to illicit crypto mining activities. Balantrapu says DeFi is vulnerable to the probability of projects turning out to be fraud or abscondment post-investment.

In our Insight section on page 44, **Sriram Tarikere**, Senior Director with Alvarez & Marsal's Global Cyber Risk Services in New York, writes about blockchain's unique security challenges/threats and the underlying infrastructure. Endpoint vulnerabilities, untested code, and third-party risks can derail any blockchain solution.

Be sure to read our Survey Report on page 72. **EC-Council's Cyber Research** cell conducted a survey to determine the state and impact of blockchain technology on businesses, their operations, and related information security. Security is seen as the direct result of blockchain implementation by nearly two-thirds of the survey respondents.

To conclude, in Sriram Tarikere's words: Blockchain is a revolutionary technology. It can completely transform insurance, banking, health care, entertainment, manufacturing, and the agricultural industry with its decentralized structure. But blindly adopting it without addressing the cybersecurity of the entire ecosystem can prove to be a critical flaw.

INDEX

Contents

3 Ways the Federal Government Is Using Technology to Advance Cybersecurity

Todd Helfrich
Vice President of Federal
Attivo Networks

When it comes to cybersecurity, the federal government is putting out fires every day — and it can be exhausting. Like most organizations, the government has traditionally defended the network perimeter firewalls and antivirus software. Unfortunately, it has become clear that adversaries have long since broken through those barriers using modern techniques such as social engineering, phishing, drive-by downloads, identity theft and impersonation.

Protecting any enterprise against today's cybercriminals — let alone nation-state threats — is a challenging task, given the volume, variety, and age of many government systems. With the rise of third-party breaches, the government needs to ensure its vendors and suppliers can protect their systems. Attivo Networks works closely with the government to help them implement innovative cybersecurity technology and steers best practices and policy conversations in a more secure direction.

Here are three government initiatives to advance cybersecurity.

1. Collaborating with Experts to Better Secure the Government and its Partners

It is important for cybersecurity organizations to be more than just manufacturers supplying technology to the government. For instance, Attivo Networks has built collaborative relationships with government agencies to help deliver more robust, more tailored solutions. This is essential in areas of critical infrastructure, intelligence, defense, and others that have specific needs that can only be addressed by a partner with a thorough understanding of the particular challenges they face and gaps they need to fill.

Information sharing has also become a priority within the government, and the recent executive order on cybersecurity emphasized the need to share threat information. Today's technology is better than ever at collecting adversary intelligence, especially when an adversary is tricked into interacting with decoy assets while safely cordoned off from the rest of the network. Studying indicators of compromise (IoCs) and the related tactics, techniques, and procedures (TTPs) and sharing that information can effectively help defenders detect and defend against specific attack tactics, even if those tactics have not yet been used against them.

Active cyber defense enables enterprises to curate relevant internal threat intelligence